Anno 9 – N.181
23 luglio/5 agosto 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Maturità... Per tutti?!?

"L'ignoranza è la notte della mente, ma una notte senza luna né stelle."
(Confucio)

Era da un po' che non trovavo spunti interessanti su cui riflettere e farmi due risate poi, come ogni anno, è arrivata la maturità...

Bello pensare a questi giovani impegnati nel primo vero esame della loro vita, la prima prova da "adulti".

Bello pensare che ci siano degli insegnanti che li hanno guidati in un percorso di crescita e poi li consegnano ad altri, ancora più preparati e disponibili, docenti che li porteranno fino al mondo del lavoro.

Bello pensare che l'illuminato Ministero della Pubblica Istruzione decida nelle tracce per i temi d'esame di inserire argomenti giovani e attuali come i social network, segno di una consapevolezza maggiore delle istituzioni rispetto alla Rete e a i suoi utenti.

Bello, sì, pensare...

Poi però mi viene in mente che ho studiato in una classe sperimentale di informatica e il computer ho dovuto imparare a usarlo da solo.
Poi però mi viene in mente che anche quelli della sezione di programmazione hanno finito le superiori nella mia stessa condizione e allora mi viene naturale chiedere ai ragazzi che conosco com'è la situazione nelle loro scuole, se usano regolarmente il PC, se hanno qualcuno di preparato che li guidi, se, insomma, qualcosa è cambiato da come mi ricordo io...

Bello pensare che le cose siano cambiate, poi però ci si sveglia tutti sudati e ci si accorge che il mondo è sempre lo stesso...

BigG

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Rapidshare & soci

Nelle ultime settimane si è registrato un sensibile incremento di file infetti originati dai cosiddetti one-click host. Secondo quanto rilevato, i criminali stanno facendo leva su servizi legali per scaricare file più popolari come Rapidshare. Di solito vengono creati dei link che rimandano a file infetti in forum piuttosto che su siti di social network. La maggior parte di questi offre tool completamente gratuiti. Attraverso questo sistema i criminali riescono a by-passare i filtri basati sul concetto di "reputazione" che inseriscono i website in "white" o "black" list. I servizi di file hosting non rientrano nelle black list e quindi non vengono bloccati. Il ventaglio di malware diffuso attraverso questo sistema è decisamente vario: ci sono backdoor, sniffer, downloader come pure diverse tipologie di Trojan e worm. Ralf Benzmueller di G Data Security Labs ha commentato: "Non è solo Rapidhsare che è stato infettato. Anche molti altri servizi di file hosting come mediafire.com, uploaded.to e uploading.com vengono utilizzati per diffondere malware". Prosegue Benzmueller: "Spesso questi file vengono pubblicizzati come l'ultima versione di un software piuttosto che come i tool più aggiornati o software craccato."
I motivi essenziali per distribuire malware attraverso servizi di file hosting deve essere analizzato da un duplice punto di vista, tecnico ed economico. L'upload di codici dannosi è per la maggior parte anonimo e i siti che offrono questo servizio garantiscono grande spazio e capacità online. Inoltre questi siti sono un modo semplice ed efficiente per distribuire malware. Questo sistema permette di evitare il controllo operato dai filtri Url che si basano sulla gestione di "white" e "black" list e quindi sulla reputazione stessa dei siti web. Vista la loro enorme popolarità questi siti di file hosting non sono inseriti in black list.

ARRIVA GOJAJAH

Chiamare all'estero spendendo quanto una telefonata nazionale. Ci sono moltissimi software di VoIP che riescono a farlo, ma la situazione cambia radicalmente quando siamo fuori casa e abbiamo solo il telefonino con noi: in quel caso le tariffe sono da capogiro. JAJAH, il popolare servizio di VoIP, e più temibile concorrente di Skype, ha inaugurato GoJAJAH, un servizio che ci permetterà di fare chiamate internazionali da cellulare, a prezzi ridicoli. Il funzionamento è semplice. Dopo esserci registrati al portale http://gojajah.com riceveremo un SMS autoconfigurante che individuerà i numeri internazionali sulla nostra rubrica. A questo punto GoJAJA associerà un numero nazionale al posto di quello internazionale, accollandosi i costi di connessione grazie alla sua rete VoIP.

jajah

IPHONE TROPPO CARI E SENZA MOTIVO

Il lancio del nuovo iPhone di Apple, in grande stile come da tradizione, ha scatenato le fantasie di milioni di utenti che però, proprio il giorno del lancio, si sono trovati a dover sborsare un prezzo superiore a quello del modello precedente per portarsi a casa il loro nuovo gioiellino. Infatti l'iPhone, sbloccato e senza abbonamento, costa la bellezza di 619 euro per la versione da 16 GB e 719 per quella da 32 GB. Un prezzo esorbitante non giustificato nemmeno dal valore dei componenti con cui è stato costruito: il famoso portale dedicato al mondo iPhone, iSuppli, si è preso la briga di smontare pezzo per pezzo il nuovo smartphone di Cupertino e di fare una stima del suo valore materiale. Il risultato è stato di 179 dollari, addirittura ben 6 dollari in più dei 174 del modello precedente... Ora, facendo due conti: 179 dollari sono circa 130 euro, quindi 719 – 130 ci porta a 590 euro che rappresenta per Apple un guadagno netto. Complimenti davvero per la politica dei prezzi... da veri strozzini!

CYBERCRIMINE: L'EUROPA AFFIDA ALL'ITALIA

Contenti loro, viene da dire! Ma in realtà è proprio così: secondo il Wall Street Journal la European Electronic Crime Task Force avrà sede a Roma e potrà avvalersi della collaborazione della polizia informatica italiana, considerata all'avanguardia nella lotta ai criminali informatici. Questa task force europea sarà comunque in costante contatto con i servizi segreti americani: l'obiettivo è quello di creare una ragnatela informatica anticrimine che permetta di segure i pirati informatici anche durante i loro spostamenti da un capo all'altro del pianeta. Una delle tecnologie utilizzate da questa task force informatica sarà il sistema di controllo antifrode dei pagamenti telematici sviluppato da Poste Italiane. Le nostre poste infatti hanno il più avanzato sistema di monitoraggio dei pagamenti elettronici che permette, a fronte di oltre 50 miliari di trasferimenti di denaro mensili, di perdere solo poche centinaia di euro: un risultato superiore a quelli ottenuti da Wall Street.

HOT NEWS

IL SOCIAL NETWORKING È MATURO!

Pochi giorni fa si è chiuso, come ogni anno, il periodo della maturità per moltissimi studenti, maturità che quest'anno ha riservato una piacevole sorpresa nelle tracce del tema d'italiano. Insieme a Svevo, alla caduta del muro di Berlino, è infatti comparso un tema d'attualità dedicato al fenomeno planetario del social networking.

La scelta del Ministero quest'anno è stata più che mai azzeccata dal momento che ormai Twitter, Facebook e affini rappresentano i principali strumenti di comunicazione giovanile e non solo. Ma Facebook è stato protagonista anche in negativo in questa maturità: già dalle 8,30 infatti le tracce degli esami erano disponibili per gli studenti su diverse pagine. Come dire: professori attenti a giocare con il fuoco o potreste rimanerci bruciati!

NOIO VOULUVANT SAVIOR...

Spesso parlare di lavoro con clienti stranieri è veramente complicato: passino coloro che parlano bene inglese che riescono a farsi capire un po' da tutti, ma se il nostro interlocutore conosce solo l'arabo il problema potrebbe essere insormontabile a meno di non avere un interprete sempre con noi.

La tecnologia però sta facendo passi da gigante e recentemente la Dial Direction di San Francisco ha presentato il primo prototipo di Sakhr Mobile S2S Translation, un rivoluzionario traduttore disponibile per iPhone e Balckberry, in grado di ascoltare le nostre frasi e tradurle in tempo reale in lingua araba. In pratica il programma utilizza una tecnologia di riconoscimento vocale in grado di capire intere frasi (anche complesse) in lingua inglese e di tradurle . Questa particolare tecnologia (che assomiglia molto al traduttore di Star Trek) potrebbe rivoluzionare il nostro modo di comunicare con persone di altri Paesi: perché, del resto, imparare le lingue quando c'è qualcuno (o meglio qualcosa) che lo fa per noi?

VIDEOGAMES

POTERE ALLE DONNE

Videogamer maschilisti preparate le armi (digitali): una schiera di donne agguerrite sta piano piano prendendo possesso dei vostri monitor.

Proprio così, da una recente indagine condotta dalla società di ricerche NDP il numero delle donne che si dilettano ai videogiochi con PC e console è aumentato notevolmente nel 2009. Nell'ultimo anno (e siamo ancora a metà) le ragazze che hanno preso familiarità con i videogames sono passate dal 23% a quasi il 30%: una crescita dovuta in gran parte alla Wii di Nintendo che ha avvicinato molto il pubblico femminile con i suoi giochi intuitivi e coinvolgenti. Ma non pensate che le ragazze si dilettino in titoli come Cooking Mama o Petz: le nuove hardcore gamers amano Call of Duty, Counter Strike e affini. Aspettatevi quindi combattimenti all'ultimo sangue: la guerra tra i sessi continua, questa volta davanti ad uno schermo...ma solo quello, per fortuna!

Cina, slitta il filtro antiporno

Una vittoria della democrazia o un problema tecnico? Forse entrambi o forse niente di tutto questo: sta di fatto che il governo cinese ha rimandato l'introduzione della legge che obbliga i rivenditori di PC a inserire nelle macchine vendute il filtro antipornografia.

Secondo le indiscrezioni riportate su alcuni blog cinesi, Green Dam Youth Escort (Diga Verde Proteggi Giovani), questo il nome del software, avrebbe grossi problemi di sicurezza che permetterebbero a pirati esperti di prendere il controllo di praticamente qualsiasi computer collegato all'Internet cinese. La verità è che l'introduzione di questo particolare filtro ha suscitato grosse polemiche all'interno degli organismi internazionali dal momento che è in grado di tracciare la lista di tutti i siti visitati da un utente e segnalarli. Una violazione della provacy intollerabile. Tuttavia molti ritengono che alla fine tutti i computer cinesi avranno la loro brava diga verde con buona pace, ancora una volta, della libertà.

CARO-TELEFONO? VIVA LA PUBBLICITÀ!

Se pensate che la vostra bolletta telefonica sia troppo salata nonostante abbiate cambiato piano tariffario centinaia di volte, allora forse un po' di pubblicità potrebbe alleggerire le vostre spese. L'operatore tedesco E-Plus ha deciso di dare un taglio alle bollette del telefonino proponendo ai suoi utenti l'invio di messaggi pubblicitari dopo telefonate e SMS. Accettando l'apposita clausola nel contratto, sarà possibile ricevere un forte sconto sulla bolletta, e perfino beneficiare di messaggi gratuiti sponsorizzati. Come dire: gli auguri di compleanno a zia Adelina sono gentilmente offerti da...

IPHONE 3GS, LO SBLOCCO È SERVITO

George Hotz è un ragazzo di 19 anni, studia e si diletta di programmazione. Tuttavia questo giovane americano è l'autentico genio che è riuscito a sbloccare il nuovo iPhone 3GS. Grazie ad un software chiamato purplera1n (purplerain per gli amici) tutti i possessori del nuovo terminale di Apple, potranno finalmente installare e utilizzare le applicazioni non autorizzate dall'App Store e che possono essere scaricate tramite il programma Cydia, una sorta di App Store alternativo. Il lavoro di GeoHotz (il suo nickname) apre la strada anche allo sblocco dei cellulari stranieri Sim-locked che ora possono essere aperti e utilizzati con qualunque sim. GeoHotz non è nuovo a questi capolavori di hacking, già a 17 anni era stato il primo a sbloccare l'iPhone EDGE. Inoltre rispetto a tutti gli altri programmi disponibili sulla Rete in grado di sbloccare l'iPhone, Purplera1n ha un altro grande vantaggio: è velocissimo. Lo sblocco del terminale avviene in meno di 2 minuti e non serve fare complicate procedure di reset o creazione di firmware personalizzati che costringono gli utenti a reinstallare applicazioni e musica ogni volta che effettuano lo sblocco.

HACKING TELEFONICO: SI BECCA 11 ANNI!

Cosa può fare un astuto hacker di 19 anni, non vedente, se gli date in mano un telefono e un computer? Fare impazzire la SWAT, la polizia speciale americana, per esempio. Matthew Weigman, nome in codice Little Hacker e un gruppo di altri amici, avevano trovato un sistema molto originale per divertirsi alle spalle di datori di lavoro, familiari, ex fidanzate ecc... Tramite un software infatti riuscivano a craccare le chiamate al 911 (il nostro 113) inviando le forze speciali, armate di tutto punto, nelle case dei bersagli delle loro burle. In questo modo sono riusciti a fregare per ben 60 volte i poliziotti che però non sono stati certo a guardare: infatti dopo una breve indagine la polizia americana è riuscita a scovare gli hacker che questa volta si sono visti arrivare la SWAT direttamente a casa loro. Ora dovranno scontare 11 anni di carcere per frode allo stato, visto che ogni intervento della SWAT costa circa 10 mila dollari. Peccato, era così divertente!

HOT NEWS

VIDEOGIOCHI COOL? L'AUSTRALIA LI CENSURA

Se vi trovate nella terra dei canguri e volete divertirvi con i vostri videogiochi preferiti, potreste avere una brutta sorpresa. Le leggi in materia di vendita e diffusione dei videogames nel continente Australiano infatti, impediscono ai negozianti di tenere sugli scaffali titoli violenti o poco adatti ad un pubblico di minori. Se siete maggiorenni la cosa non cambia: la violenza è completamente bandita dai videogames. Le nuove regole imposte dal governo di Sidney sui videogiochi comprendono anche moltissimi titoli online e persino alcuni giochini in flash che si trovano su molti portali dedicati all'intrattenimento videoludico. Tra i capolavori digitali bloccati dalla censura ci sono anche Crysis, Fallout 3, Painkiller e molti altri... in compenso se volete potete sfidare i vostri amici in lunghe partite a Teddy, l'orsetto tenerone. Il divertimento è assicurato!

SIGARETTE ONLINE A PREZZI BASSI.. MA È REATO!

Il prezzo delle sigarette sale e la recessione avanza? Beh, perché allora non farsi una bella scorta sul web? Del resto i negozi online vendono tutto a prezzi più bassi... Così molti fumatori esasperati dai continui aumenti si sono rivolti al sito svizzero K2Smokes.ch dove era possibile acquistare sigarette a prezzi molto contenuti. Una grande idea... illegale: la legge in Italia non prevede la commercializzazione al di fuori delle tabaccherie che pagano una tassa allo Stato.

BENTORNATO STEVE JOBS!

Una notizia che ha ben poco a che vedere con l'hacking ma sicuramente ha molto a che vedere con la storia della tecnologia come la conosciamo oggi. Steve Jobs, CEO e co-fondatore di Apple, è tornato al lavoro dopo la lunga e faticosa lotta contro un tumore al pancreas che lo aveva ridotto praticamente uno scheletro. A gennaio, con una lettera ai dipendenti e agli azionisti, Jobs aveva annunciato che per un semestre sabbatico avrebbe pensato esclusivamente alla sua malattia abbandonando la guida di apple nelle mani del suo vice Tim Cook. Promessa mantenuta: a metà di giugno è arrivato l'annuncio del ritorno del Re al vertice di Apple. Jobs in un primo momento lavorerà part-time durante il periodo estivo, per poi tornare in grande stile verso la fine di agosto con un evento che, a quanto pare, servirà per presentare i nuovi iPod Touch dotati di fotocamera digitale e, si vocifera, navigatore GPS.

NON C'È INTERNET? ALLORA VAI DI SMS!

Google, in collaborazione con l'operatore MTN Uganda e la fondazione Grameen ha inaugurato in Africa un nuovo sistema per fornire alcuni servizi Web in zone non ancora raggiunte dalla rete UMTS o telefonica. Come? Utilizzando gli SMS! Si tratta di un progetto molto ambizioso e sicuramente di grande impatto sociale che ha come obiettivo quello di ridurre lo svantaggio tecnologico in zone dove i problemi sono molto più seri dell'assenza di internet. I servizi offerti al momento sono due Google Trader e Google Tips: il primo permette alle persone dotate di cellulare di richiedere l'acquisto di un bene sul web semplicemente scrivendo nei 160 caratteri il nome o la descrizione del prodotto che desidera. Sarà Google a ricevere il messaggio e a metterlo in contatto con il venditore simulando quello che può essere il contatto con un negozio online. Il secondo servizio Google Tips, sostituisce il motore di ricerca vero e proprio: è possibile chiedere di tutto, dalla data della scoperta dell'America al macellaio più vicino. La risposta, chiaramente, arriverà al destinatario via SMS.

SPECIALE HACKER JOURNAL

The Pirate Bay

...la resa

Alla fine ce l'hanno fatta le Major

Ebbene sì, quando ho letto la notizia un po' mi è venuto il magone. Vedere che uno dei baluardi della neutralità della rete ha dovuto cedere alle pressioni di Major è stato duro. Ma cosa è successo di preciso ai ragazzi della Baia? Dopo aver subito la sconfitta al famoso processo ed essere stati condannati a pagare 30 milioni di corone (2,7 milioni di euro) di danni e interessi all'industria del disco, del cinema e dei videogiochi, hanno visto in pericolo il sito stesso. Davanti al rischio di dover chiudere www.thepiratebay.org hanno preferito cederlo alla Global Gaming Factory X, azienda che gestisce numerosi internet café nel mondo. Il proprietario, Hans Pandeya, ha dichiarato che intende dare una svolta al portale cercando una soluzione: "in modo che i fornitori di contenuti e i detentori di copyright siano pagati per quello che è scaricato dal nostro sito". Il solo leggere queste dichiarazioni getta nella disperazione più profonda chi aveva visto nella Baia uno strenuo difensore della libera diffusione delle idee. Possiamo capire che Peter e soci si siano trovati veramente a corto di ossigeno dopo il processo e preferiscano vedere il sito evolversi in termini commerciali piuttosto che chiuso, ma a noi resta il rimpianto per una "fort Alamo" che non c'è stata. Apprezziamo molto il fatto che la Baia abbia deciso di utilizzare i circa 5,6 miliodi di euro della vendita per costituire una fondazione a difesa della libertà d'espressione nella rete ma certo non sarà come leggere il loro blog ogni giorno con i post di scherno verso gli uffici legali delle Major e sicuramente il nuovo titolare del sito deve mettere in conto un crollo dei contatti che potrebbe scalzare thepiratebay.org dalla lista dei 100 siti più visitati. Ci mancherà la nostra baia preferita.

Fredrik Neij, 30 anni, Gottfrid Svartholm, 24 anni, Peter Sunde, 30 anni e fondatore di Pirate Bay hanno venduto il famoso sito.

TUTTA LA VERITÀ ...e la sòla

Alla fine abbiamo perso noi

Il 17 aprile si è concluso il processo a The Pirate Bay con la condanna dei quattro imputati, Fredrik Neij , Gottfried Svartholm, Peter Sunde e Carl Lundström per violazione del diritto d'autore. Durante il processo abbiamo ascoltato dichiarazioni nobili "La violazione del diritto d'autore è solo una conseguenza sfortunata della libertà di condivisione offerta da The Pirate Bay" sosteneva Peter Sunde, dichiarazioni ironiche "Dove sono i miei 10 milioni? Per favore, dove sono finiti?" si chiedeva Svartholm Varg; e a processo finito dichiarazioni di speranza "Come in tutti i film, gli eroi perdono all'inizio ma trionfano alla fine. È l'unica cosa che Hollywood ci abbia insegnato". Bravi ragazzi, tenete duro, siamo con voi. Il primo luglio una breve, sintetica notizia ha cambiato come dire… il punto di vista: La Baia venduta per 5,6 milioni euro. 5,6 milioni di euro, questo è il valore della libertà di condivisione. O almeno quello che i campioni di Pirate Bay gli attribuiscono. E così abbiamo scoperto

I nostri eroi giungeranno finalmente a Hollywood. Non da vincitori sulle spoglie delle Major sconfitte ma da ricchi turisti.

dov'erano i milioni che cercava Varg e ancora cosa intendevano per "trionfare alla fine". Certo, il tesoretto non lo intascano loro ma una fondazione che si occuperà di alimentare progetti dedicati alla tutela dei diritti digitali. Dove sarà la sede di questa fondazione? Isole Cayman? Bahamas?
Li abbiamo sostenuti con passione, vi abbiamo chiesto di seguirci in questa crociata e ora è giusto fare ammenda. Ci siamo lasciati affascinare dalla battaglia di Davide contro Golia, dalla lotta alle Major, dalla difesa della libertà su Internet, e così facendo abbiamo trascurato alcuni non trascurabili particolari ma ora il gioco è finito. Hanno creato un sistema per scaricare materiale protetto da Copyright, l'hanno fatto crescere e l'hanno venduto. In perfetto stile New Economy, tanto di cappello, ma niente di più.

FIREFOX, nuovo capitolo

Un motore rinnovato sotto un cofano vecchio che, però, risulta ancora un passo avanti i suoi concorrenti

Da un bel po' di tempo si parlava dell'introduzione in Firefox di una serie di funzioni tanto avanzate quanto poco utili per gli utenti. Per questo motivo, l'uscita del nuovo Firefox 3.5 ha rappresentato un annuncio tanto atteso quanto temuto. Da una parte si attendeva una risposta al nuovo Internet Explorer mentre dall'altra si temeva uno stravolgimento del browser, con conseguenti problemi di adattamento e pesantezza.

:: Velocità, pura velocità

Contrariamente a quanto alcuni temevano e altri speravano, il nuovo Firefox 3.5 sembra proprio il gemello della sua versione precedente: nessuna funzione spettacolare, nessuna fantastica aggiunta all'interfaccia utente e nessun problema d'uso. Contrariamente alla sfida lanciata da IE sulle nuove funzioni, lo staff di Firefox ha preferito insistere dove il concorrente mostrava il suo punto debole più eclatante: la velocità. Velocità di caricamento, velocità di rendering dei siti, velocità di utilizzo, di apprendimento. Il nuovo vecchio Firefox è stato dotato di un motore nuovo fiammante, ottimizzato per fornire una velocità nettamente superiore alla versione precedente e per restare il più aderente possibile agli standard del Web. Ovviamente, il miglioramento ha visto coinvolto soprattutto il sistema di gestione di Javascript, un punto su cui i browser hanno sempre avuto qualche problema.

Non è un caso che Firefox sia uno dei pochi programmi ad avere una community di fan come gli artisti: l'arrivo di questo browser ha rappresentato una rivoluzione.

Il nuovo TraceMonkey risulta tra i motori javascript più veloci in assoluto, ben oltre le prestazioni della già veloce vecchia versione di Firefox.

:: Multimediale!

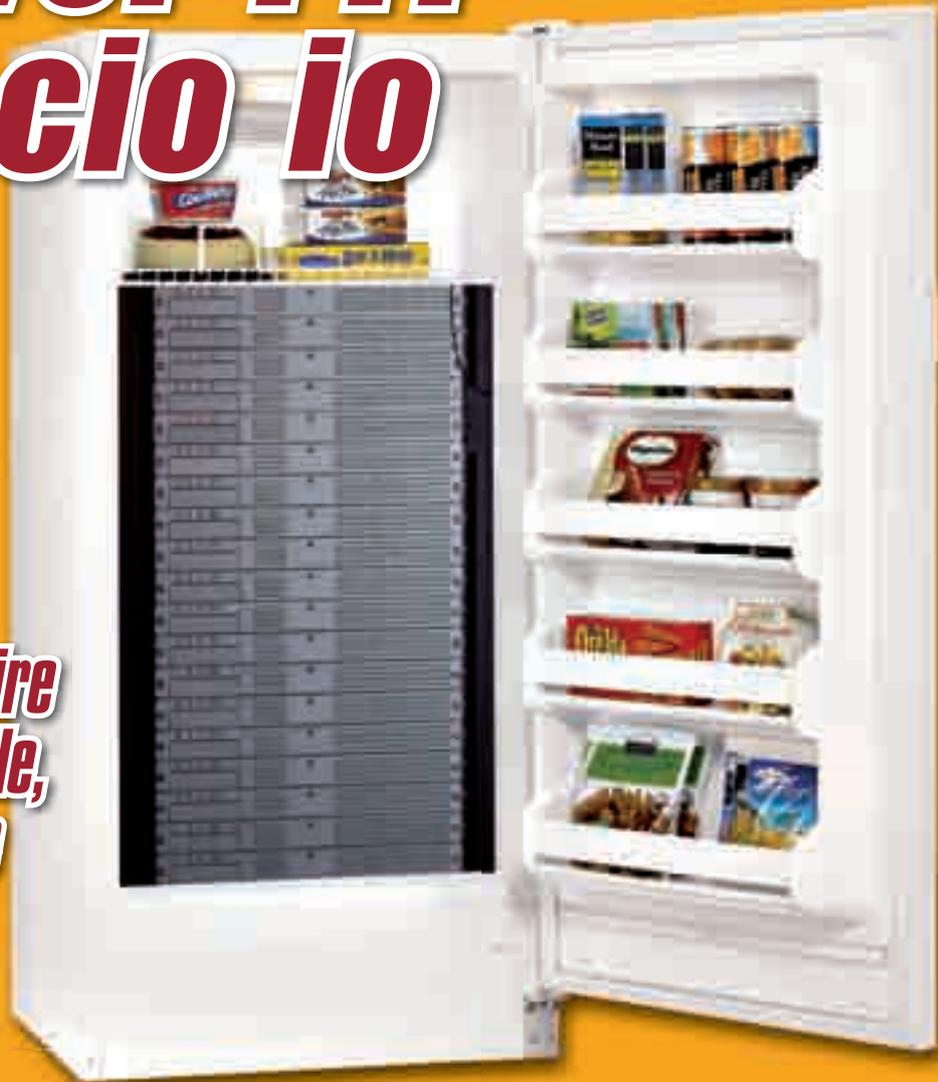
Questa ricerca della prestazione, ovviamente, non è stata fine a se stessa: Firefox 3.5 permette ora di accedere a diversi elementi multimediali online senza l'aggiunta di plugin. Questo permette agli sviluppatori Web di utilizzare materiale audio e video, basato su standard Open Source, con la certezza di offrire esperienze coinvolgenti e immediate ai loro utenti e senza costringerli a scaricare alcun add-on oppure perdite di prestazioni causate dall'interfacciamento tra browser e plugin. Un primo passo, necessario, verso una maggior integrazione e una standardizzazione dei formati che vedrà certamente Mozilla tra i protagonisti. Dopotutto, quella di Firefox è una proposta molto interessante ma bisognerà vedere quanti sviluppatori seguiranno il suggerimento e useranno veramente elementi in questo formato nelle loro pagine. La collaborazione degli sviluppatori si rende indispensabile e interessante anche per un altro motivo: l'inserimento di queste funzioni permette agli elementi multimediali di interagire realmente con l'utente, senza limitarlo al controllo di riproduzione o del volume. Staremo a vedere come verrà sfruttata questa possibilità. Una innovazione attesa e già vista in via embrionale nelle versioni precedenti, invece, è la possibilità di navigare in modo anonimo. Firefox 3.5 include una modalità di navigazione che ci assicura di non inviare alcun dato privato sul Web, di tutelare al massimo i cookie presenti sul PC e di impedire qualsiasi tipo di raccolta dati delle nostre abitudini. Una funzione che si è sviluppata notevolmente rispetto al passato ma che, alla luce dei problemi di privacy che gli attuali siti web pongono, risulta sempre più sentita. Un'esigenza che si esprime anche nell'inserimento di una nuova funzione che permette di chiedere al browser di "dimenticare" un sito. Alla sua attivazione, ogni traccia sul computer della navigazione su un certo sito (e solo su quello) viene eliminata totalmente e definitivamente. Un discorso simile alla cancellazione di cronologia e cookie ma mirata su un target specifico. Meno specifica ma comunque interessante è, invece, la possibilità di eliminare con un clic la cronologia recente, altra caratteristica volta a tutelare la privacy dell'utente e dedicata a chi vuole cancellare sessioni di surfing sulla Rete, lasciando intatte le altre preferenze.

:: Ti trovo...

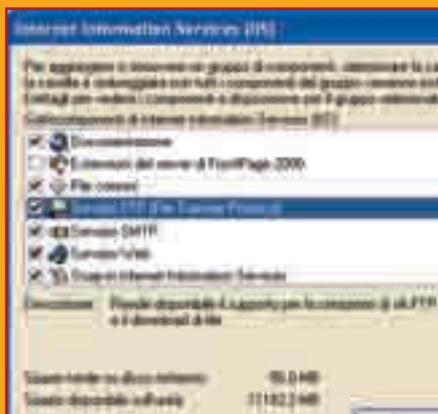
Ultima funzione minore aggiunta è quella dedicata alla geolocalizzazione: con l'autorizzazione dell'utente e visitando siti che fanno uso di questa tecnologia, Firefox può fornire direttamente informazioni sulla nostra posizione dello spazio. Una funzione che potrebbe essere un problema per la privacy personale, certo, ma anche una funzione estremamente utile in campo mobile (ma non solo). Pensiamo alla comodità di collegarci a un qualsiasi sito di mappe e vedere istantaneamente la nostra posizione, di ordinare una pizza e finire direttamente sul sito dell'azienda che consegna nella nostra zona e così via. Ovviamente, la sfida è simile a quella posta con l'inserimento di controlli multimediali: se verrà raccolta da un numero sufficiente di sviluppatori Web, potrebbe rivoluzionare il modo in cui funzionano i servizi geografici sul Web.

L'annuncio dell'uscita di Firefox 3.5 è arrivato ai vecchi utilizzatori tramite Firefox stesso. Chi non l'avesse lo può scaricare da www.mozilla-europe.org.

Il server FTP lo faccio io

Se cerchiamo un sistema che consenta di trasferire facilmente grandi file, perché non pensare a un server FTP domestico?

Installare in casa un server FTP non è per niente un'operazione complessa, anzi basta il software giusto (senza spendere un centesimo, naturalmente) e pochi accorgimenti che vedremo a breve.
La questione è: perché dovremmo avere un server FTP in casa?
Il perché lo dice il nome stesso del servizio: File Transfer Protocol – protocollo per il trasferimento di file. Un server FTP si comporta come un disco remoto, da cui possiamo prelevare file e a cui possiamo inviare file, cosa che per esempio non è prevista dal semplice HTTP senza un'adeguata programmazione del sito (e comunque le possibilità sono molto limitate).
Il fatto che sia un protocollo espressamente dedicato a questo servizio comporta molti vantaggi, tra i quali la ripresa dei trasferimenti interrotti e maggiori velocità degli stessi, banda disponibile permettendo. Ora, gli scenari possibili sono diversi, ognuno può implementare il proprio server FTP per il motivo che crede più opportuno, ma (hint) un'area privata in casa nostra a cui possono accedere i nostri amici dall'esterno è un'ottima soluzione al problema del trasferimento di grandi file che difficilmente possono essere inviati via mail o via messenger. A buon intenditor...

:: Problemi da risolvere

Per prima cosa, dobbiamo scegliere il software che costituirà il nostro server FTP: va scelto naturalmente in base al sistema operativo che gira sulla macchina destinata a questo compito, e a questo proposito è opportuno fare qualche considerazione. Innanzitutto, non è vero che chi usa Windows piuttosto di Linux parta svantaggiato, perché per entrambi è facile trovare software FTP in tutte le salse. Inoltre, se proprio non vogliamo installare software di terze parti sul computer, possiamo installare quello predefinito del sistema, cioè

Internet Information Services è presente sul CD originale di Windows ma non viene installato automaticamente.

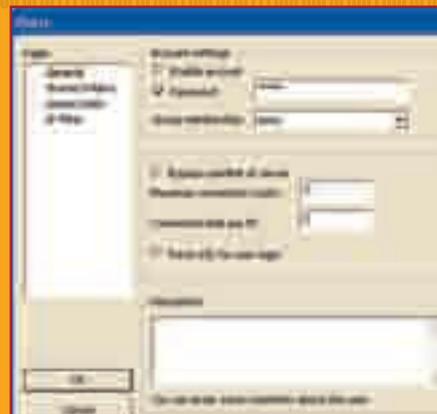
IIS per Windows XP Professional e, in Linux, il daemon incluso nella distribuzione scelta. Ma questo forse è il minore dei problemi, perché alla fine si riduce il tutto a scegliere il programma con cui ci troviamo meglio. Ciò che invece deve essere analizzato a dovere è come permettere agli utenti esterni di raggiungere il server, in quanto esistono due scogli da superare: il fatto di avere un IP pubblico che ci viene assegnato dinamicamente dal nostro provider al momento della connessione e il solito problema di dirottamento della comunicazione dal router al PC su cui effettivamente gira il software server.

:: Configuriamo IIS

Internet Information Services non fa parte della configurazione standard di Windows XP Professional, ma è presente sul CD e può essere installato sul computer attraverso lo strumento Installazione componenti di Windows. Dovremo selezionare Internet Information Services (IIS) e poi fare clic su Dettagli, perché il servizio FTP non è selezionato automaticamente e dobbiamo farlo a mano. Terminata la procedura, troveremo sul disco C: una nuova cartella chiamata Inetpub. Questa contiene tutte le cartelle necessarie per il funzionamento di IIS, tra cui ftproot, quella che per impostazione predefinita è dedicata a contenere i file resi disponibili dal server FTP. Possiamo cambiare questa impostazione da MMC: facciamo clic destro sull'icona di Risorse del computer, scegliamo Gestione, poi apriamo Servizi e applicazioni, Internet Information Services, Siti FTP e facciamo clic destro su Sito FTP predefinito. Nella finestra di dialogo mostrata potremo anche definire le modalità di accesso al server. Consentendo l'accesso anonimo, verrà usato l'utente predefinito di Windows per operare sulle cartelle FTP; chi ha remore per quanto riguarda la sicurezza farebbe bene a disattivare la condivisione semplice delle cartelle, creare un nuovo utente solo per l'accesso FTP e usare quello per l'accesso anonimo, in quanto quello proposto (IUSR_nome-computer) è quello creato da Windows anche per le operazioni del server Web. I permessi di accesso e operativi per i singoli utenti, invece, sono definiti nelle opzioni della cartella (clic destro sulla cartella stessa e comando Condivisione e protezione del menu contestuale): dopo aver creato un utente Windows per ogni amico a cui vogliamo concedere l'accesso, possiamo inserirli tutti in un gruppo apposito e assegnare a questo il livello di operatività che desideriamo (solo lettura, oppure lettura e scrittura per consentire l'upload dei file).

La configurazione di accesso di IIS non è delle più semplici, ma il software è compreso in Windows ed è comodo.

:: FileZilla è anche server

Lo conosciamo tutti come client, ma il progetto FileZilla produce anche un buon server FTP, sempre gratuito e Open Source,

La configurazione avviene senza problemi per FileZilla Server, che è un software gratuito e Open Source.

che gira perfettamente in Windows. Se la procedura di configurazione di IIS ci è sembrata troppo complessa, possiamo tagliare la testa al toro, come si suol dire, e scegliere questo programma, che dispone di una propria interfaccia di gestione con cui aggiungere e configurare utenti e permessi è veramente semplicissimo. Una volta creata la struttura di cartelle per il server FTP e installato il programma, possiamo creare un gruppo di utenti (Edit/Groups) a cui assegnare una cartella root e i permessi adeguati, poi creare i singoli utenti (Edit/Users) da assegnare al gruppo, ognuno con la propria password.

:: L'accesso dall'esterno

Normalmente disponiamo di un router collegato a Internet che fa da gateway per la rete, attraverso il quale passano anche le comunicazioni dall'esterno verso l'interno. Dobbiamo configurarlo in modo che le porte 20 e 21 siano aperte e reindirizzate verso il computer su cui gira il server FTP (con il port forwarding o NAT, come viene designato in certi modelli), o nessuno lo vedrà in linea. Risolto questo problema, dobbiamo pensare all'indirizzo corrispondente al nostro server. Mentre nella rete locale va fissato un IP statico per il computer con tale compito, il nostro provider ci assegna un IP dinamico ogni volta che ci colleghiamo, conviene quindi creare un account su servizi come no-ip.com o dyndns.com.

Milano-Seattle in ¼ di secondo

Un viaggio quasi alla velocità della luce tra cavi e server: il volto nascosto di Internet.

Se cerchiamo un libro su Amazon, per prima cosa apriremo il browser e scriveremo l'indirizzo del sito, www.amazon.com, nella barra degli indirizzi. Il nostro sistema operativo, in collaborazione con il browser, preparerà una richiesta, un pacchetto di dati. Questa verrà inviata, tramite la nostra connessione, al server DNS impostato durante la configurazione della connessione a Internet o fornito automaticamente dal Provider. Lo scopo di questo server è di tradurre il nome mnemonico che abbiamo digitato in un indirizzo IPv4: una sequenza di 4 numeri da 0 a 255 che identifica univocamente ogni computer collegato alla Rete. In alcuni casi la traduzione fornirà un indirizzo IPv6: di diverso formato, questo indirizzo ha le stesse funzioni di quello IPv4 ed è la sua recente evoluzione. Una volta ottenuto l'indirizzo del server che voglaimo visitare, tramite un pacchetto di informazioni inviato dal DNS, il nostro sistema operativo provvederà a costruire un nuovo pacchetto di dati che invierà ancora al nostro provider. Questo pacchetto conterrà la richiesta di ricevere la pagina specificata nel browser oppure quella di default del sito e sarà destinato al server corrispondente all'indirizzo fornito dal DNS.

:: Passaparola

Il nostro provider accoglierà questo pacchetto, come già aveva accolta la richiesta fatta al DNS, tramite un computer preposto al collegamento con gli utenti oppure tramite un router con funzioni equivalenti. In ogni caso, il pacchetto di informazioni verrà controllato e, in base all'IP del destinatario, diversi dispositivi del provider lo inoltreranno sulla Rete. A questo punto sono possibili tre diversi scenari. Se il pacchetto con la richiesta è indirizzato a un server sulla rete del nostro stesso operatore, sarà totalmente compito del nostro provider recapitarlo. Se la destina-

zione è sulla rete di un diverso provider con cui il nostro ha accordi di scambio di dati alla pari, il pacchetto verrà indirizzato a un NAP tra il nostro operatore e quello di destinazione. I NAP sono nodi di interscambio tra diversi operatori e permettono i passaggi dati da uno all'altro: sono punti critici di Internet e, di solito, gli operatori ne hanno diversi sparsi sulle loro reti. Se l'operatore di destinazione ha un NAP in comune con il nostro, il pacchetto gli arriverà attraverso questo NAP. Se manca il NAP, invece, il pacchetto verrà dirottato sulla rete di uno o più operatori intermedi, fino a raggiungere un NAP di ingresso alla rete del destinatario. Una volta arrivato alla rete a cui appartiene anche il server da raggiungere, il pacchetto viene consegnato dai router dell'operatore alla sua destinazione. A questo punto, i dati nel pacchetto verranno letti ed elaborati dal server destinatario. Nel caso di richiesta di pagina Web, questa verrà inserita in uno o più pacchetti che verranno rispediti al mittente originario usando metodi del tutto simili. In genere, ogni pacchetto contiene pochi Kb di dati e le informazioni di grandi dimensioni vengono spezzettate in frammenti, così da renderne più facile la trasmissione e il transito dalle apparecchiature di rete. Ovviamente non si tratta di uno smembramento arbitrario dei dati: il metodo usato è tale che il computer destinatario può ricostruire facilmente l'informazione originale partendo da tutti i pacchetti che gli sono arrivati.

:: Velocissimo

Il meccanismo, apparentemente così complicato, funziona a una velocità enorme: da Milano a Seattle bastano da 200 a 300 millisecondi. La riprova è alla portata di chiunque: basta aprire un prompt dei comandi DOS e digitare il comando ping, seguito dal nome del sito che vogliamo raggiungere. Questo creerà un pacchetto dati di dimensioni standard che verrà spedito a destinazione e a cui il server risponderà con un altro pacchetto: il confronto tra i tempi di transito ci permette di trovare la velocità di trasmissione. Velocità così elevate, capaci di passare

Il DSLAM permette di raggruppare più linee con un numero di cavi inferiore. Se è presente non possiamo avere velocità elevate.

attraverso le reti dell'intero pianeta in meno di un secondo, sono dovute a una infrastruttura molto evoluta, creata negli anni dai diversi provider. Infrastruttura che si compone spesso di componenti impensabili, come i numerosi cavi sottomarini che collegano diverse nazioni del mondo, che attraversano gli oceani e permettono diversi tipi di comunicazioni.
L'osservazione del transito dei dati da un punto di vista fisico è affascinante quanto il punto di vista logico. Una volta partiti dal nostro computer, i dati arrivano via cavo o tramite Wi-Fi a un dispositivo che li trasforma, permettendone il transito su una rete diversa dalla LAN casalinga. Questo viene chiamato modem, adapter o, generalmente, HAG. Se siamo abbonati FastWeb, per esempio, compito dell'HAG sarà quello di tradurre gli impulsi elettrici della LAN in un formato ottico, adatto alla fibra. Lo stesso concetto vale per chiunque, persino per chi usa Internet "senza fili" tramite il cellulare: c'è sempre un HAG, sotto forme diverse, che trasforma i segnali per farli arrivare a uno degli hub del nostro provider.
A volte succede che, per questioni tecnologiche, siano presenti anche altre apparecchiature che, tuttavia, rallentano le prestazioni delle connessioni: nel caso di molte linee ADSL, per esempio, vengono usate particolari apparecchiature (chiamate DSLAM) per convogliare più segnali in un unico doppino in rame, grazie a una tecnica chiamata multiplexing. Nel caso di linee HDSL, invece, le velocità dalla centrale del provider all'utenza risultano maggiori perché il segnale non viene mescolato con altre linee: il doppino parte dall'utente e arriva alla centrale, dove vi sono gli hub degli operatori, senza intermediari. Una volta arrivato all'hub del nostro operatore, il segnale viene smistato tramite la sua rete verso altri hub oppure a destinazione: come già accennato, la sua strada viene decisa dai router in base all'indirizzo di destinazione di ogni pacchetto. Nell'ipotesi di una comunicazione con server di altre reti, il segnale verrà inviato dall'hub locale a un altro hub su cui confluiscono altri hub simili al primo. Da qui, il segnale potrà passare a un altro hub minore oppure essere inviato ad altri hub superiori oppure a un NAP e così via, secondo una struttura gerarchica tipica di ogni operatore. Fisicamente, questi collegamenti sono realizzati tramite fibra ottica ma non è obbligatorio: per la sua stessa natura, Internet funziona raggrup-

Le torrette e gli armadi di Telecom contengono permutatori come questi: collegano i fili di casa con quelli delle centrali.

QUESTO ARTICOLO...

Perché scrivere un articolo di questo genere su Hacker Journal? Dopotutto diciamo cose che che dovrebbero essere chiare a qualsiasi nostro lettore. Il fatto è che in redazione abbiamo letto l'articolo intitolato "Milano-Seattle 1/2 secondo", pubblicato su Focus numero 201 di Luglio. Abbiamo pensato che una rivista "scientifica" e "seria" potesse insegnarci qualcosa, magari darci qualche spunto per approfondimenti. Invece abbiamo iniziato a ridere perché il numero di imprecisioni e di ingenuità contenute in queste 5 pagine andava oggettivamente oltre ogni possibile svista editoriale: capita anche a noi di sbagliare ma riuscire a fare un articolo che sembra provenire da un altro pianeta è una cosa che non siamo mai riusciti a realizzare e abbiamo avuto persino il sospetto che fosse un articolo dedicato al primo aprile. Invece no. Lungi da noi l'idea di correggere una rivista certamente più seria e attendibile della nostra... O forse no?

pando sono un'unica struttura logica reti fisicamente molto differenti. Nei meccanismi P2P, per esempio, potremmo avere un segnale casalingo ADSL che poi passa su diverse fibre ottiche, attraversa l'oceano in un cavo (sempre in fibra), viene trasferito tramite un doppino telefonico in rame e finisce sul computer destinatario tramite un Wi-Fi casalingo.

:: Non solo hub!

In aggiunta ai sistemi di collegamento per gli utenti, la rete di ogni provider è quindi composta da "super hub" che mettono in collegamento tra loro queste strutture "di prima linea". In più sono presenti diversi server usati per i compiti più disparati: DNS, proxy, server di autenticazione, antivirus, sorveglianza delle connessioni e via dicendo. Rendersi conto del viaggio avventuroso dei dati attraverso la rete è tutto sommato facile: basta usare il comando giusto. È lo scopo del comando Tracert, di funzionamento simile al ping: ogni apparecchiatura attraversata dalla comunicazione, si identificherà restituendo un pacchetto di dati al mittente. Partendo dalla rete di Tiscali di Milano, un semplice comando Tracert ci segnala che un pacchetto dati partito da un computer della nostra LAN, aziendale, arriva all'adattatore ADSL del nostro ufficio e viene instradato verso l'hub di zona di Tiscali. Da qui, tramite fibra ottica, viene rilanciato da un hub all'altro, per 3 volte, nella rete Tiscali, fino ad arrivare all'hub nazionale dell'operatore.

Una volta arrivato viene nuovamente instradato, tramite fibra ottica e attraverso una dorsale di comunicazione europea, verso Francoforte, dove viene ricevuto da un hub della rete del provider tedesco Teleglobe. Il router di contatto con Tiscali di Teleglobe lo rimanda, poi, a un altro router dello stesso operatore, dedicato ai collegamenti transoceanici. I dati passano poi attraverso uno dei tanti cavi sottomarini che collegano Europa ed USA, ricevuti da un altro router a New York. Una volta negli USA, il viaggio prosegue tramite le reti di altri operatori, sulle dorsali di comunicazione americane, verso Chicago e arriva fino a Seattle, all'ingresso nella rete di Amazon. Qui viene, finalmente, smistato a destinazione, dopo 16 passaggi complessivi. Naturalmente, a seconda della disponibilità di collegamenti, i router possono scegliere strade diverse per ogni pacchetto di dati. Inoltre, grazie alle elevatissime capacità di elaborazione dei router usati (milioni di pacchetti contemporanei), alla potenza dei server coinvolti nel procedimento, alla possibilità di modulare segnali digitali trasmessi in fibra aumentandone la densità, il mondo intero è a portata di mano in frazioni di secondo.

La Fui Lai è una nave che può posare fino a 3200 tonnellate di cavo per volta. Grazie a navi come lei Internet è così veloce.

Uno schema, parziale, dei collegamenti in arrivo, dai NAP, a Google. È uno dei siti più frequentati al mondo ed è normale che veda coinvolti tanti ISP di livello globale.

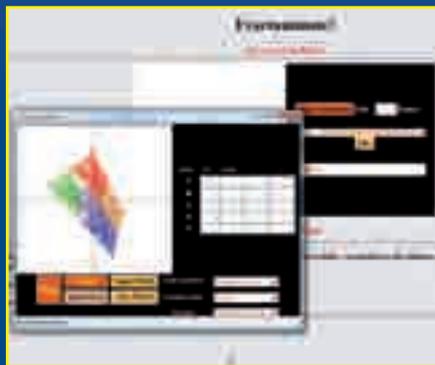
CRITTOSOLUZIONE

Nel box a pagina 13 del numero scorso abbiamo spiegato che le pagine 12 e 13 erano pensate come un gioco che permettesse di leggere un articolo, cifrato, sulla crittografia a partire dalla Bibbia fino ai giorni nostri. C'è un sistema di cifratura usato nella Bibbia, nel libro di Geremia, per codificare le parole Caldei e Babele: l' Atbash. È un cifrario di sostituzione monoalfabetica in cui l'ordine delle lettere è rovesciato. Decifrando la prima parte dell'articolo si fa menzione a una potenza militare del mondo occidentale antico: Roma. Il secondo paragrafo dell'articolo è stato codificato con il cifrario di Cesare: consiste nello spostamento dell'alfabeto di un numero di lettere pari alla chiave. Il passo in più necessario alla decodifica era quello di capire la chiave usata: uno spostamento di 7 lettere. Decodificando questo brano si ricevevano indizi su un cifrario polialfabetico attribuito erroneamente a Vigenere. La sfida si faceva più interessante: evoluzione del cifrario di Cesare, quello di Vigenere prevede che ogni lettera venga cifrata con diversi alfabeti, determinati da una parola chiave. La parola chiave era proprio "vigenere" e si poteva giungere alla soluzione con l'uso di un programma di calcolo statistico e un minimo di conoscenze tecniche. Nel testo facevamo riferimento al tentativo di Baudot di codificare le lettere in un formato simile all'attuale ASCII: si tratta di un codice a 5 bit studiato per l'uso telegrafico, decisamente più pratico dell'alfabeto Morse. Il sistema di decrittazione consisteva semplicemente nel capire il metodo usato e interpretare il testo tramite una delle tante tabelle di corrispondenza disponibili in Rete. Una decifrazione di tutto riposo per prepararsi al passaggio successivo: la prima macchina Enigma. Nel testo facevamo riferimento alla prima versione della macchina cifrante tedesca e al nome di Turing. La rimessa in chiaro del testo era possibile solo dopo un certo lavoro di crittoanalisi. Il brano di testo decodificato in precedenza parlava di un Enigma a 4 rotori e dava anche la chiave necessaria per la decodifica: il nome di Turing, "Alan". L'ultima parte del testo è stata cifrata usando un sistema simile al moderno RSA ma abbiamo fatto in modo che le soluzioni per la decodifica potessero essere due. Abbiamo numerato le lettere dell'alfabeto e le abbiamo cifrate usando un algoritmo RSA le cui chiavi sono state generate usando come numeri primi il 23 e il 37. Un sistema semplice, quindi, che poteva essere facilmente abbattuto grazie all'intuizione: la codifica di lettere singole ci fa ricadere nel caso dei banali cifrari monoalfabetici. Malgrado avessimo suggerito un grado di difficoltà elevato, l'intero testo poteva essere decodificato grazie all'analisi statistica della distribuzione delle lettere. Per finire non resta che parlare dell'ultimo livello di codifica, con un messaggio al di fuori del testo. Come abbiamo suggerito con l'immagine iniziale dell'articolo non era altro che un messaggio scritto in Braille, usando una notazione inversa dallo standard. Il Braille, infatti, si scrive da destra a sinistra e si legge sull'altro lato del foglio, da sinistra a destra. Noi ci siamo limitati a nascondere i punti nella pagina e a scrivere normalmente da sinistra a destra. Proprio vero che non c'è peggior cieco di chi non vuol vedere.

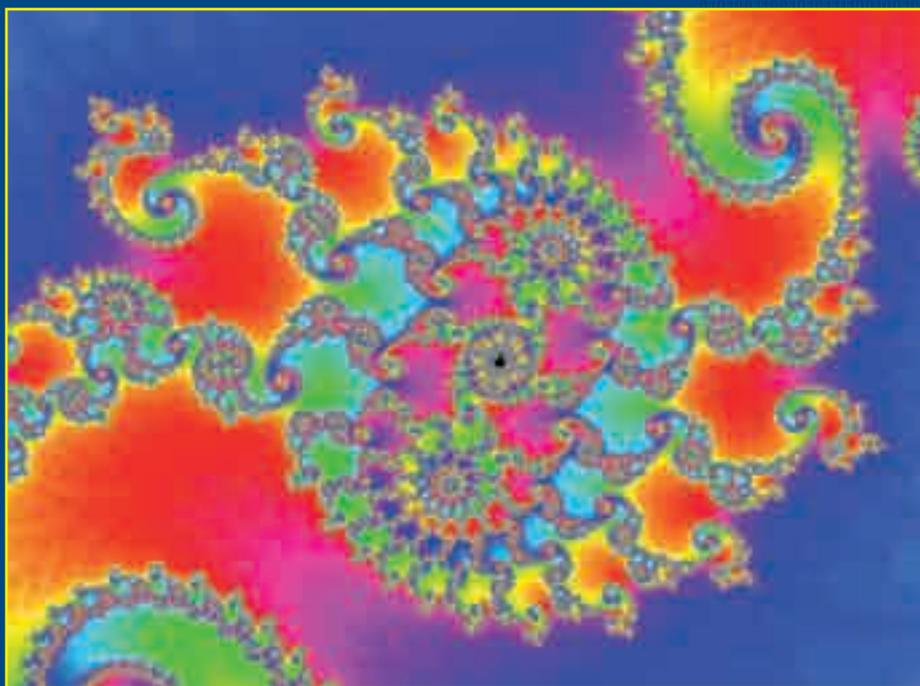
Non era troppo difficile risalire al contenuto dell'articolo cifrato pubblicato nel numero scorso. Bastava armarsi di pazienza e fare attenzione agli indizi di ogni brano.

I frattali sono probabilmente gli oggetti matematici più affascinanti e vengono comunemente usati per rappresentare la realtà

OGGETTI SPEZZATI

Immaginiamo di voler misurare la lunghezza delle coste italiane usando un compasso con l'apertura di 1 km. Ora misuriamo i punti di intersezione tra i cerchi di misura e la costa per trovarne la lunghezza. Cambiamo scala usando un compasso con un'apertura di 10 metri e ripetiamo la misura. Ovviamente avremo molti più cerchi ma, meno ovviamente, la somma delle misure fatte sarà superiore a quella precedente. Potremo fare altre prove, con scale minori o inferiori, scoprendo che riducendo sempre più le distanze tra le punte del compasso, la somma delle misure risulterà in crescita. Questo fenomeno è tipico di molte strutture naturali ma anche di figure matematiche uniche: i frattali. Una figura frattale è definita come qualcosa che su scale diverse ha una struttura ricorsiva. In ambito naturale, oltre alle coste, sono frattali anche gli alberi (ogni ramo ha una struttura simile a quella dell'insieme di cui fa parte), le montagne, alcuni organi di esseri viventi e altro ancora.

Molti programmatori amanti della grafica si occupano di frattali. Anche sul Web.

:: Questione di matematica

Il termine frattale venne inventato nel 1975 da un matematico francese di origini polacche: Benoît Mandelbrot. Il suo merito fu quello di riprendere il lavoro del matematico francese Julia e di dargli una nuova dimensione grazie all'utilizzo di tecniche di calcolo elettronico: diversamente da Julia, che compiva le sue osservazioni con metodi tradizionali, Mandelbrot decise di affidarsi a un computer per

L'esplorazione di un frattale è un viaggio affascinante che coinvolge la matematica ma che ha un'applicazione pratica nella rappresentazione della realtà.

poter ottenere una rappresentazione grafica di un algoritmo in sostituzione delle classiche rappresentazioni di funzioni. Per ottenere una geometria frattale è necessario definire un algoritmo di calcolo che viene reiterato sul prodotto dell'applicazione precedente per un numero congruo di volte. Ad ogni iterazione, il risultato si avvicina sempre più al risultato finale che, tuttavia, non esiste: il numero di iterazioni possibili è arbitrario e dipende solo dalle capacità umane o della macchina usata. Per fare un esempio, pensiamo di disegnare un triangolo equilatero su un foglio (prima iterazione). Poi dividiamolo in modo da ottenere 4 triangoli identici tra loro (seconda iterazione). Ora dividiamo ognuno dei triangoli ottenuti in modo da ottenerne altri, con lo stesso sistema (terza iterazione). Ripetendo in continuazione questo procedimento, otterremo una figura frattale, tra l'altro realizzabile nelle prime fasi anche manualmente. Da matematico, Mandelbrot si occupò soprattutto di numeri complessi, arrivando a scoprire quasi per caso che la rappresentazione grafica di un'applicazione ricorsiva di una formula particolare a un insieme di numeri complessi aveva l'aspetto di un frattale.

[Formula di Mendelbrot]

$$a_n+1=a^2_n+P_0$$

dove a_n e P_0 sono numeri complessi

L'applicazione ricorsiva di questa formula, rappresentata su un piano cartesiano, è visibile come sfondo in apertura di questo articolo e non a caso si tratta di un'immagine piuttosto famosa, nonché di una tra le più affascinanti. Dal punto di vista strettamente grafico, il colore viene ottenuto indicando ogni punto diversamente in base ai risultati dei calcoli e sulla base di un numero di iterazioni prefissato.

:: In pratica...

Se desideriamo iniziare ad esplorare i frattali, basta una rapida ricerca con Google per imbattersi in programmi disponibili per qualsiasi piattaforma e con qualsiasi tipo di licenza: dall'open source allo shareware. In generale sono tutti adatti, anche considerando che le operazioni matematiche da svolgere per rappresentare i frattali sono complesse ma rapidamente eseguibili da qualsiasi computer. Per questo motivo, diversi programmi non solo permettono l'esplorazione del frattale di Mandelbrot ma anche di molti altri. Molto interessanti da usare come guide per l'esplorazione, invece, sono le innumerevoli gallerie di immagini curate da scienziati e appassionati: per la loro natura pressoché infinita, i frattali sono tutt'ora oggetto di studio e curiosità. Dal punto di vista pratico, invece, le tecniche sviluppate hanno permesso di trovare nuovi metodi di rappresentazione della realtà e sono usate in programmi di grafica 3D, film e videogame. In quest'ultimo campo, gli studi frattali hanno acquisito un valore economico: la possibilità di poter dare alcune istruzioni di base e iterarle per arrivare a formare alberi, erba, peli e quant'altro ha permesso alla grafica di arrivare, oggi, a sorprendere: un passaggio dal realistico al reale.

NUMERI COMPLESSI

Un numero si definisce complesso se è la somma tra un numero reale e uno immaginario. I numeri immaginari, rappresentati dalla lettera i, vengono indicati come "la soluzione dell'equazione x2 + 1 = 0", che equivale a dire:

$$x2 = -1$$

$$x = \sqrt{-1}$$

Usando solo numeri reali, tale equazione non ha alcuna soluzione perché non esiste alcun numero reale che, elevato al quadrato, possa risultare -1.

Risposta sbagliata. Ovvero, perché controllare l'esattezza dei dati è indispensabile

Ahi ahi ahi, signora Longari...

In programmazione, qualunque sia la piattaforma per cui si sta sviluppando, va posta particolare attenzione sul controllo della validità dei dati. Si tratta spesso di una scocciatura, che ci costringe a scrivere molto codice in più che non ha diretta influenza sul funzionamento del programma, ma che (è proprio il caso di dirlo) spesso ci salva la paga, se non il posto di lavoro. Niente di più imbarazzante, infatti, di un programma stiloso che però non calcola bene un valore a causa di un inserimento errato, specialmente se lo stiamo mostrando al capo.

:: Quel dato è il mio tipo

I linguaggi di programmazione vengono classificati in livello, in base alla maggiore o minore vicinanza a quello base, che è costituito dal codice di programmazione nativo del processore e che si basa sulle sole istruzioni elementari che il processore stesso è in grado di interpretare ed eseguire (per intenderci, è il formato dei file eseguibili che sono, per l'appunto, direttamente eseguibili dalla macchina). I linguaggi di basso livello sono quelli più vicini al linguaggio macchina, come Assembly e C, mentre quelli più ad alto livello sono quelli che, mediante astrazioni e regole semantiche più simili a quelle umane, sono stati studiati per rendere più facile il lavoro del programmatore (i linguaggi più ad alto livello sono il BASIC, il PROLOG e il FORTH). Generalmente, il dato viene trattato diversamente in base al livello del linguaggio: quelli con più alto livello sono più rigidi dal punto di vista della gestione del tipo di dato, mentre i linguaggi di livello più basso sono più elastici e consentono più facilmente il passaggio di dati tra variabili non omogenee tra loro. Quindi, mentre in BASIC ci pensa il compilatore ad avvisarci della cosa segnalandola come errore, in C si presume che sia il programmatore a occuparsi delle verifiche del caso: senza questo accorgimento, ci potremmo ritrovare dopo diversi passaggi con una variabile contenente un tipo di dato sbagliato perché convertito automaticamente dal compilatore in un passaggio precedente all'errore, che dovremo poi scovare e correggere. La regola generale è che una variabile usata in un'operazione deve contenere un dato di tipo adeguato a quella operazione e, mentre la logica di questo assunto è lapalissiana, non sempre ci si accorge per tempo di errori di tipo, specialmente lavorando con linguaggi di basso livello.
La verifica di un dato, però, non è limitata all'accertarsi che sia del tipo ade-

guato, ma anche che sia coerente nella forma. Facciamo un esempio: se un programma deve inviare un'email, occorre che l'indirizzo del destinatario sia scritto nella maniera corretta. Se lasciamo fare al compilatore, si limiterà a verificare che si tratti di una stringa, ma non potremo lamentarci se l'invio non va a buon fine perché l'indirizzo non contiene la chiocciola.

:: Procedure di validazione

Per essere certi che il flusso del programma non venga interrotto da un errore provocato da una variabile di tipo sbagliato, occorre quindi accertarsene mediante funzioni appositamente programmate. Il vantaggio di perdere un po' di tempo scrivendole non si limita però a evitare errori di programma, perché dovremo farlo una volta sola: se le salviamo in una nostra libreria potremo poi sfruttarle tutte le volte in cui si rende necessario controllare la validità di un dato. In Codice 1 troviamo un semplice esempio: la validazione di un indirizzo email in PHP, che si limita a verificare la correttezza sintattica ma non la sua esistenza. In Codice 2, invece, una procedura controlla se il carattere battuto dall'operatore è una cifra o una lettera. Sulla falsa riga di queste procedure, possiamo creare funzioni che controllino la validità di una data, che verifichino che un numero sia compreso in un determinato range, che si accertino

Controllo numero o lettera in C++

```
#include<iostream>
usingnamespace std;
#include<string>

int main()
{
  char y; cout << "Enter a character or
number: _\b"; cin >> y; if(!isdigit(y))
    cout << "It's a Letter";
  else
    cout << "It's a Number";
  cout << '\n'; return 0;
}
```

Controllo indirizzo email in PHP

```
<?php
function valid_email($email) {
 if (!ereg("^[^@]{1,64}@[^@]{1,255}$", $email)) { return false; }
 $email_array = explode("@", $email);
 $local_array = explode(".", $email_array[0]);
 for ($i = 0; $i < sizeof($local_array); $i++) {
   if (!ereg("^(([A-Za-z0-9!#$%&#038;'*+/=?^_`{|}~-][A-Za-
z0-9!#$%&#038;'*+/=?^_`{|}~\.-]{0,63})|(\"[^(\\|\")]{0,62}\"))$",
$local_array[$i])) { return false; } }
 if (!ereg("^\[?[0-9\.]+\]?$", $email_array[1])) {
  $domain_array = explode(".", $email_array[1]);
  if (sizeof($domain_array) < 2) { return false; }
  for ($i = 0; $i < sizeof($domain_array); $i++) {
   if (!ereg("^(([A-Za-z0-9][A-Za-z0-9-]{0,61}[A-Za-z0-9])|([A-Za-z0-9]+))$",
$domain_array[$i])) { return false; } } }
 return true; }
?>
```

dell'esistenza di un file sul disco e così via, secondo le nostre necessità. Dobbiamo poi inserirle in modo che controllino il dato immesso prima che venga dato in pasto a qualunque altra procedura: se il test passa, il dato è ok e può essere girato alla funzione successiva per l'elaborazione; se il test non passa si stampa un messaggio di errore e si permette all'utente di tornare indietro e ripetere l'inserimento.

:: Perché controllare

Il fatto che sia importante controllare la validità dei dati per evitare errore di programma l'abbiamo già chiarito, ma non è tutto qui ciò che è da prendere in considerazione. Se si ferma un programma perché tenta di dividere un numero con una lettera, poco male, facciamo solo una brutta figura. Ma in certi casi errori come questo possono costituire vere e proprie falle di sicurezza. Un puntatore calcolato male può causare l'insorgere di eccezioni che, se non gestite a regola d'arte, possono dare il controllo della macchina a un malintenzionato mediante l'esecuzione di codice arbitrario iniettato con un inserimento dati ad hoc (pensiamo a tutti gli errori di buffer overflow corretti nel tempo in Internet Explorer, per esempio). Ogni programma in cui è richiesto l'inserimento di dati manualmente da parte di un operatore, quindi, deve essere assolutamente blindato per quello che riguarda il controllo delle immissioni. Sembra una sciocchezza ma non lo è per niente.
La stessa cosa può dirsi per il Web: gli script PHP o ASP (o scritti in qualunque altro linguaggio per il Web) devono contenere forti funzioni di validazione dei dati, perché tecniche di attacco come SQL Injection e Cross-Site Scripting si fondano proprio sulla speranza che il programmatore non sia stato sufficientemente attento nella verifica dei dati inseriti attraverso un modulo.

:: Conclusioni

La verifica dei dati e dei tipi di dati deve essere uno dei punti fondamentali della check-list del programmatore. Ogni volta in cui si maneggia un dato, anche creato dal programma, è opportuno implementare una procedura di controllo del tipo, mentre nel caso di inserimenti manuali è sempre meglio aggiungere anche una verifica di conformità del dato immesso. Un accorgimento forse un po' noioso e a volte lungo da implementare, ma che ci libererà da tanti grattacapi che potrebbero altrimenti verificarsi.

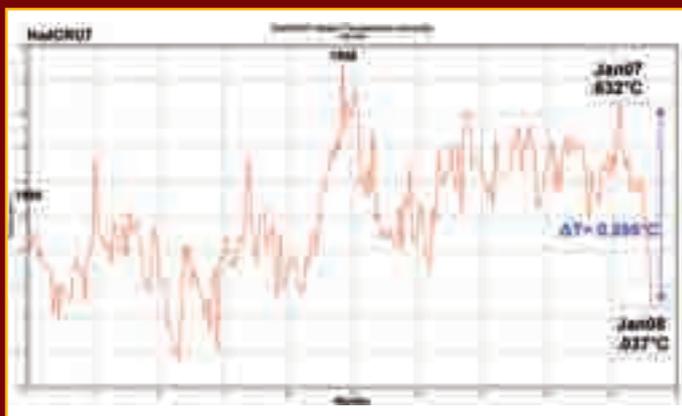
Nella vita non esiste solo il bianco e il nero

0 Sfumature 1

Su che base decidiamo che una maglietta è pulita? La domanda non è pretenziosa e la risposta è piuttosto complessa: le moderne lavatrici adeguano il loro ciclo di pulizia al livello di sporco dei capi e fornire una risposta precisa significa ridurre i costi di milioni di lavaggi giornalieri. Solo che la risposta è quanto meno complicata. Se considerassimo pulita una maglietta del tutto priva di macchie, anche microscopiche, il ciclo di lavaggio dovrebbe durare qualche giorno ed essere fatto in ambienti sterili. Viceversa, possiamo definire pulita una maglietta macchiata?

:: Logica e insiemi

Quesiti come questi fanno riflettere perché in un mondo in cui le cose vengono analizzate sulla base di dati certi, sul bit, sul bianco e nero, ogni possibile soluzione che non rientra in questi schemi è quasi un disturbo. Il problema è stato brillantemente risolto con il ricorso a un nuovo modello di logica che estende quello tipico della logica booleana (tanto caro agli informatici): la logica fuzzy (sfumata). La rivoluzione consiste nel definire ad ogni proposizione un grado di verità compreso tra 0 e 1 senza limitarsi a questi due estremi, come avviene nella logica booleana.

Riprendendo l'esempio della nostra maglietta, potremmo dire che questa può essere sufficientemente sporca da dover essere lavata oppure abbastanza pulita da essere indossata, usando una scala che in questo caso è personale. Nel caso delle lavatrici "intelligenti", la scala viene fissata dal costruttore e si basa su rilevamenti di sensori ma il concetto è lo stesso: non esiste più il bianco e nero, il pulito e lo sporco ma ci sono una serie di sfumature che si avvicinano più a una condizione che all'altra. In matematica, questo concetto è espresso tramite la generalizzazione $\mu F(p)$, dove p è il predicato, F è l'insieme fuzzy e μ è il valore di appartenenza corrispondente al predicato. L'aspetto più affascinante di questa struttura logica è meglio percepibile se la si tratta dal punto di vista degli insiemi. Per prima cosa occorre considerare che l'attribuzione di un grado di verità a ogni proposizione invalida il principio di non contraddizione. Mentre nella logica classica un elemento che appartiene a un dato insieme, A, non può appartenere all'insieme !A (non-A), la logica fuzzy rivoluziona il concetto: lo stesso elemento può essere contenuto nell'intersezione di entrambi gli insiemi e muoversi dall'uno all'altro in funzione

Le previsioni del tempo e l'evoluzione climatica sono due ambiti in cui la logica fuzzy risulta indispensabile per poter formalizzare le osservazioni e passare alla rielaborazione dei dati.

In borsa, la logica fuzzy viene usata per predire l'andamento del mercato. I sistemi più seri sono in grado di mostrare un andamento predittivo con un margine di errore ridottissimo.

del grado di verità che gli viene attribuito. Questo concetto, ovviamente, rivoluziona completamente il funzionamento degli operatori logici a cui ci si è abituati con l'uso della logica booleana.

:: Si, no, forse... Boh?

Nello specifico, la logica booleana definisce l'operatore NOT come una negazione di una proposizione. Una condizione che non è definibile con lo stesso senso nell'ambito della logica fuzzy. In questo ambito, l'operatore NOT non agisce più solo sui predicati ma sul valore di attendibilità che gli viene attribuito. Per fare un esempio chiarificatore, se affermiamo che una maglietta è sporca al 30%, annotabile come 0,3F(sporca), l'applicazione dell'operatore NOT trasformerà questa affermazione in "una maglietta è non sporca al 70%": !0,3F(sporca)=0,7 F(!sporca).

Allo stesso modo occorrerà intervenire anche sugli altri operatori booleani per fargli acquisire una funzionalità differente all'interno di un contesto logico differente. L'operatore AND, per esempio, equivale al valore minimo del grado di verità degli elementi inclusi in entrambi gli insiemi considerati mentre l'operatore OR corrisponde al suo valore massimo. Le variazioni nei processi logici che conseguono da queste modifiche sono sostanziali e possono diventare estremamente complesse ma la loro importanza è enorme per una grande quantità di scienze in cui la contrapposizione tra vero e falso è una semplificazione troppo schematica: climatologia, economia, intelligenza artificiale, sociologia e via dicendo. Dal punto di vista informatico, una implementazione di base di sistemi basati sulla logica fuzzy prevede che non si possano più trattare proposizioni come vere o false.

Risulta quindi necessario corredarle di un indice di attendibilità che le faccia rientrare in un ambito logico in cui non ha più senso parlare di una dicotomia ma sia più appropriato usare locuzioni come "simile a", "vicino a" e via dicendo. Il tipo di dati più facilmente assimilabile a questo comportamento è quello percentuale ma occorrerà trattarlo come dato complesso, unendo un tipo percentuale a un tipo adatto all'affermazione, per poter distinguere i dati tra loro e, da lì, derivare le equivalenze e le operazioni necessarie. Un passo importante dell'implementazione, infatti, consiste proprio nel definire gli insiemi sovrapponibili di valori. Un esempio semplice da comprendere, riprendendo la questione del bucato: affermare che una maglietta è pulita al 30% è equivalente all'affermare che è sporca al 70%. Due affermazioni che umanamente sono facilmente comprensibili ma che richiedono una formalizzazione complessa e una strutturazione dei dati adeguata, oltre a un certo lavoro di programmazione per trattare le relazioni fuzzy: del tutto aliene alla logica booleana dei nostri computer ma indispensabili per avvicinarsi alla realtà.

FUZZY NON E' STATISTICA

Non confondiamo la logica fuzzy con la statistica perché sono due cose diverse: trattano aspetti diversi a diversi livelli. La differenza è facilmente comprensibile se si pensa a 100 bottiglie d'acqua di cui 5 sono avvelenate. La statistica ci dice che il 5% di quelle bottiglie contengono veleno. La logica fuzzy subentra, invece, quando andiamo a definire cos'è una bottiglia avvelenata: una che contiene una percentuale infinitesima di veleno, nell'ordine dei miliardesimi di litro, è avvelenata? Oppure una che contiene più veleno che acqua?
Unendo la logica fuzzy e la statistica, tuttavia, si ottengono risultati interessanti, praticamente e matematicamente. Se definiamo come avvelenata una bottiglia il cui contenuto di veleno sia pari a una particella su un milione e quel 5% di bottiglie rientra e non supera questa casistica, l'insieme dell'acqua a nostra disposizione, mescolata in un contenitore da 100 litri, risulta non avvelenata perché presenta una quantità di veleno statisticamente identica ma molto vicino all'insieme dell'acqua pulita.

Ma quanto peso???

Sembra una domanda facile ma apre la porta a mille riflessioni che ci riguardano da vicino

Ieri sera ho deciso di mettermi a dieta, sapete com'è, l'età avanza, le ginocchia cigolano e allora ho preso questa triste decisione. Stamane mi sono svegliato risoluto nel portare avanti questa mia battaglia con i chili di troppo e sono salito sulla mia bilancia elettronica per vedere da dove partivo, risultato: 105 Kg... Speravo meno ma va bene, allora si comincia, vado in farmacia a prendere delle barrette sostitutive e già che ci sono mi peso anche lì: risultato 112 Kg... E no!!! A questo punto diventa una questione di principio, i miei genitori abitano davanti alla farmacia e decido di salire da loro e provare la loro bilancia, risultato 99 Kg... Se proprio devo scegliere...
Insomma, le mie buone intenzioni si sono infrante contro l'impossibilità di stabilire con precisione quanto peso, così sono andato ad informarmi: un chilogrammo è esattamente la massa di un decimetro cubo di acqua distillata alla temperatura di 4 °C, per molto tempo (dal 1889), e per rendere più facili le cose, si è utilizzato come campione primario del peso un cilindro di platino e iridio che si avvicinava il più possibile al decimetro cubo di acqua distillata e che da allora viene conservato presso il Bureau International des Poids et Mesures di Sèvres, in Francia. Tutti i Paesi che vogliono un sistema proprio di riferimento devono farsi fare una copia di quel cilindro. Ma anche questo sistema non funziona visto che il campione di riferimento ha subito variazioni in tutti questi anni. Sono punto e a capo.

Questa è una ricostruzione digitale del Chilogrammo Campione, in Italia è conservato presso il Ministero dell'industria.

Chi potesse risincronizzare a suo piacere tutti gli orologi del globo sarebbe l'uomo più potente al mondo.

:: Non solo peso

A questo punto mi viene in mente che non è la prima volta che nella mia vita mi scontro con questo problema a cui è ora di dare un nome: CALIBRAZIONE. Tutti abbiamo scattato delle foto in vacanza, oppure all'ultimo concerto, scatti bellissimo, con colori fantastici... sul display della macchina fotografica, poi torniamo a casa, li scarichiamo sul PC e vediamo tutt'altro. Ma non è finita, una volta che provassimo a stampare la stessa foto otterremmo un risultato diverso. Non siamo calibrati, la nostra macchina fotografica, il nostro PC e la nostra stampante hanno un "concetto di chilogrammo" diverso, in questo caso possiamo dire che hanno una calibrazione cromatica diversa.
Certo, per i sistemi informatici esistono profili colore e tarature dei monitor molto più facili da applicare rispetto al mio "problema di peso".

Anche il metro di riferimento ha subito, nel corso degli anni, un accorciamento.

Tra l'altro lo stesso tipo di problema è riscontrabile nelle misure di lunghezza dove il metro campione si è accorciato. Una cosa invece che siamo bravissimi a misurare è la temperatura, difatti il termometro al mercurio è molto preciso... peccato che ormai sia illegale, almeno nella comunità europea, e così ci ritroviamo sotto le ascelle simpatici oggettini in plastica con tanto di display che ci danno temperature a caso.

:: Sincronizziamo gli orologi

Alla fine della mia giornata dedicata alle misurazioni mi sono ritrovato con un paio di amici a mangiare qualcosa, tanto l'idea della dieta è ormai saltata, e tra un birra e una fetta di pizza si è affacciato un altro affascinante scenario. Mettiamo caso, non tanto lontano, che

Le attuali livelle laser usate nei cantieri hanno una tolleranza di circa il 10%, molto meno le vecchie livelle a bolla.

tutti gli apparecchi di misurazione del tempo siano collegati all'orologio mondiale e quindi sempre sincronizzati ad esso. Ora, mettiamo che ci sia un operatore che controlla il corretto funzionamento dell'orologio e decida che vuole accorciarsi il turno. Ora, in questo scenario, l'operatore dell'orologio sarebbe probabilmente l'uomo più potente al mondo... Pensate se ogni turno lui spostasse avanti le lancette di 5 minuti, in 288 ci avrebbe portato avanti di un giorno intero, un giorno perso nel nulla. Certo il panorama è assolutamente surreale ma, almeno a me, agli amici presenti, alla pizza e alle birre è sembrato rivelatore di una più profonda verità.

I lati della base della piramide di Cheope sono pressoché perfettamente dritti, con una tolleranza media di meno del 2%

:: Il filo di gesso

"La matematica procede per affinamento" diceva la mia prof del liceo e poi aggiungeva: "siamo esseri razionali e ragionevoli, se dividendo i tre un conto da 10.000 lire (ndr: qua rivelo la mia età) razionalmente sappiamo che ognuno di noi dovrebbe mettere 3.333,33333 periodico lire ma,essendo ragionevoli, uno metterà 3.334 lire e la faccenda si risolve". Beh! Aveva ragione lei.
Da sempre l'uomo cerca più cifre del π, da sempre cerchiamo l'unità di misura di riferimento che non possa subire variazioni, cerchiamo numeri primi sempre più grandi e via così ma volendo ben vedere una livella laser utilizzata oggi, ultimo grido della cantieristica, ha una tolleranza del 10% mentre ogni lato della base della piramide di Cheope ha una tolleranza di meno del 2%.
A questo punto, è ormai notte e tutti i miei buoni propositi di dieta stanno annegando in una lattina di Coca, ho imparato due cose:
1° - Una bilancia è più che sufficiente per essere ragionevolmente sicuri che la settimana dopo segnerà il mio calo di peso.
2° - È ora che io smetta di cercare scuse per non iniziare la dieta.

BigG

Il tesoro dei pirati

Si chiama Oak Island, e da più di due secoli nasconde un misterioso tesoro. Sarà veramente così?

Si trova nella contea di Lunenburg in Nova Scotia ed è collegata alla terraferma da un ponte di poco più di un chilometro. È una delle trecento isolette della Baia di Mahone, la più vicina alla terraferma, misura un chilometro e mezzo circa di lunghezza per 800 metri di larghezza. Ricca di calette, in passato è stato un approdo sicuro per equipaggi di navi pirata, soprattutto inglesi e spagnole. Nel 1795 inizia la storia che ha portato alla ribalta questo pezzo di terra sconosciuto: un ragazzino, Daniel McGinniss, trova un affossamento circolare nel terreno. Un po' per gioco un po' trascinato dalla magia dei racconti sui pirati, insieme a due amici inizia a scavare e trova, a due piedi di profondità, una pavimentazione in pietra. Rimossa la pavimentazione continua lo scavo e dopo 10 piedi (3 metri circa), trova una seconda pavimentazione, in legno di quercia. L'isola si chiama Oak Island, ma di querce non ce ne sono. Non più almeno. Lo scavo procede di altri 10 piedi, altra pavimentazione in quercia, ma la curiosità dei ragazzini si ferma. Troppa fatica per trovare solo terra e legno. Può bastare. Torneranno allo scavo in età adulta, 8 anni dopo, nel 1803, come operai della Onslow Company, una compagnia finanziata da Simeon Lynds, un appassionato di misteri e di tesori. Lo scavo ricomincia e procede rapidamente. Ogni 10 piedi c'è il solito pavimento di quercia ma non solo: a 40 piedi viene trovato uno strato di carbone, a 50 uno di stucco e a 60 uno di fibre di cocco intrecciate. Un materiale strano da trovare sull'isola (non è una zona di palme da cocco) che veniva utilizzato sulle navi, dalla metà del 1600 circa, per impermeabilizzare i carichi preziosi. Pirati. Chi altri avrebbero potuto pensare e realizzare un opera del genere? Lo scavo continua, lì sotto c'è un tesoro. Finalmente, a 90 piedi, la prova tangibile che l'impresa non è campata per aria: una pietra, piatta, basalto (anche questa non reperibile nell'arco di miglia e miglia) con un'incisione cifrata.

La riproduzione della scritta cifrata trovata sulla lastra di pietra a 90 piedi di profondità. La traduzione ufficiale è Forty Feet below two million pounds are buried, ma se vogliamo essere precisi c'è qualcosa che non va: il triangolo con I tratti trasversali è di troppo.

:: Una cassaforte "naturale"

L'incisione viene decifrata da un professore dell'università di Halifax: Forty Feet below two million pounds are buried, quaranta piedi più giù sono sepolti due milioni di sterline. Ci siamo. Lì sotto c'è un tesoro, basta scendere di altri 40 piedi e il gioco è fatto. E invece no: tolta la pietra e il pavimento di quercia su cui poggiava accade l'imprevisto. Il mattino dopo, tornando al lavoro, gli operai trovano lo scavo pieno d'acqua. Tentano di vuotarlo con dei secchi, ma il livello non scende. Si scava un pozzo parallelo, ma a 90 piedi anche questo si riempie d'acqua. L'impresa viene abbandonata. Nel 1849 la Truro Company arriva alla fossa con una trivella da perforazione petrolifera, inizia a bucare e aggiunge mistero al mistero. Perfora qualcosa che sembra essere una cassa di legno contenente metallo (schegge di legno e fibra di cocco rimangono attaccate alla punta della trivella) e va oltre, più in profondità. Trovando altre pavimentazioni di quercia e terreno non compatto. Pare non avere fondo. Decisa a recuperare il tesoro, inizia a pompare l'acqua con macchinari industriali. Il livello cala, per poi risalire… al ritmo della marea. Nella vicina baia Smith's Cove, distante 500 piedi dal Money Pit (il pozzo del denaro), l'acqua ribolle, uscendo letteralmente dal fondale in almeno cinque punti vicini alla spiaggia. Sorpresa delle sorprese: la baia è artificiale. I punti in cui l'acqua ribolle sono l'ingresso dei canali di inondazione del pozzo. Ogni bocchetta è stata sigillata con fibra di cocco, per far passare l'acqua e filtrare sabbia e detriti, in modo da non intasare i condotti. Un sistema ben congegnato: togliendo il "tappo" costituito dalla pavimentazione in quercia posta a 90 piedi, la Onslow Company aveva fatto scattare il meccanismo di sicurezza della cassaforte.

L'ingresso del Money Pit oggi. I lavori sono fermi; nel pozzo, nel corso dei vari tentativi di arrivare al tesoro, sono morte 18 persone.

Le vie di accesso dell'acqua vengono chiuse ma il mare continua a entrare. Ci sono altri canali, ma non ci sono più soldi per cercarli. L'avventura della Truro Company finisce qui. Altre compagnie hanno tentato la via del pozzo nel corso degli anni, ma tutte senza successo: dal 1861 ci ha provato la Oak Island Association, dal 1893 la The Oak Island Treasure Company che ha trovato, nei pressi del pozzo, il frammento di una seconda roccia incisa, oltre a manufatti, arnesi, monete, cocci di vasi di porcellana e terracotta, frammenti di oggetti in oro. Un falso o un'altra clamorosa svista dei ricercatori passati? Dagli inizi del 900 molti personaggi illustri, tra cui il futuro 32esimo presidente statunitense Franklin Delano Roosevelt, hanno tentato l'infruttuoso assalto al tesoro. Il tesoro, se esiste, è ancora là. Oggi l'isola è privata e l'attuale proprietario ha chiesto un finanziamento di 12 milioni di dollari allo stato canadese per riprendere gli scavi.

:: Il codice

La lastra cifrata originale (se è mai esistita), vera o falsa che fosse,non c'è più; così come sono spariti molti manufatti trovati durante gli scavi. Per la cifratura del messaggio è stato utilizzato un semplice codice per sostituzione. Il codice scelto risulta un po' troppo semplice, sempre che sia stato decifrato correttamente. Si è supposto che la lingua del messaggio fosse l'inglese sulla base dell'unità di misura delle distanza tra i pavimenti di quercia. La distanza è espressa in piedi, unità di misura anglosassone, quindi la lingua del messaggio è l'inglese. È veramente così? La decrittazione potrebbe anche essere corretta,

L'esterno del pozzo. Sullo sfondo si vede la Smith's Cove, dalla quale si diramano i condotti di allagamento del Money Pit.

ma nella prima parola è stato omesso un carattere: secondo il professore è stato scritto per errore e poi cancellato con due tratti trasversali. Ora, tutto è possibile, ma siamo in presenza di un'isola trasformata in una cassaforte naturale perfetta, con studi applicati di alta ingegneria idraulica e meccanica portati a termine con una tecnologia inesistente per l'epoca e il genio che ha concepito tutto questo sbaglia a scrivere la seconda lettera del messaggio? Poco plausibile. Lasciamo a voi il messaggio cifrato, magari… chissà, noi, pirati del nostro tempo, riusciremo a risolvere l'enigma lasciatoci dai nostri precursori di trecento anni fa!

Colleghiamoci da remoto al PC con una console di terminale

SSH, un terminale remoto criptato

Uno strumento rapido ed efficiente per gestire una macchina da remoto è il terminale: grazie ad esso, infatti, possiamo controllare completamente un PC occupando una ridotta quantità di banda nella connessione. Per far uso di un terminale remoto, però, il vecchio protocollo Telnet è sconsigliato, dato che non fornisce nessuna cifratura dei dati in transito da un sistema all'altro. È preferibile quindi impiegare SSH, un sistema client-server che permette di stabilire delle connessioni criptate tra le macchine. Vediamo quindi in questo articolo come installare e configurare al meglio OpenSSH, un'implementazione opensource del protocollo SSH. Come sistema operativo di riferimento adotteremo la distribuzione GNU/Linux Ubuntu 9.04.

:: Installazione di SSH

Per maggiore chiarezza, chiamiamo A il PC che vogliamo raggiungere dalla rete e B il PC che vogliamo usare per collegarci al primo. Sulla macchina A, quindi, andremo ad installare il pacchetto per l'applicazione server di SSH: avviamo su questo PC una finestra di terminale (se usiamo il desktop Gnome andiamo sul menu Applicazioni e clicchiamo su Accessori > Terminale) e lanciamo il comando "sudo apt-get install openssh-server". Sulla macchina B, poi, assicuriamoci che sia installato un client SSH: se su questa è presente una distribuzione derivata da Debian (come, appunto, Ubuntu) eseguiamo il comando "sudo apt-get install openssh-client".

:: Password contro criptografia asimmetrica

Nella configurazione di default, SSH permette di accedere al sistema remoto tramite password. Un metodo di autenticazione più sicuro, però, consiste nell'utilizzo di un sistema di criptografia asimmetrica basato sull'adozione di una coppia di chiavi, una chiave privata e una pubblica: la chiave privata non viene divulgata all'esterno, mentre la chiave pubblica viene condivisa con i sistemi sui quali vogliamo ottenere l'accesso. Per sfruttare questa modalità di autenticazione, quindi, dobbiamo creare la coppia di chiavi sul PC B e poi esportare solamente la chiave pubblica sul PC A.

```
ale@pitagora:~$ sudo apt-get install openssh-server
[sudo] password for ale:
Lettura della lista dei pacchetti in corso... Fatto
Generazione dell'albero delle dipendenze in corso
Lettura informazioni sullo stato... Fatto
Pacchetti suggeriti:
  rssh molly-guard openssh-blacklist openssh-blacklist-extra
I seguenti pacchetti NUOVI (NEW) saranno installati:
  openssh-server
0 aggiornati, 1 installati, 0 da rimuovere e 0 non aggiornati.
È necessario prendere 0B/285kB di archivi.
Dopo quest'operazione, verranno occupati 782kB di spazio su disco.
Preconfigurazione dei pacchetti in corso
Selezionato il pacchetto openssh-server, che non lo era.
(Lettura del database ... 152217 file e directory attualmente installati.)
Spacchetto openssh-server (da .../openssh-server_1%3a5.1p1-5ubuntu1_i386.deb) .
```

Sul PC che vogliamo controllare da remoto installiamo l'applicazione server di OpenSSH.

:: Creiamo le chiavi

Sul computer B generiamo dunque le chiavi per l'autenticazione. In una console di terminale lanciamo il comando "ssh-keygen -t dsa". Ci verrà chiesto in quale file vogliamo salvare la chiave privata; premiamo semplicemente Invio per confermare la scelta di default, ~/.ssh/id_dsa. Poi indichiamo la passphrase: si tratta di una lunga password che ci verrà richiesta per decriptare la chiave privata, operazione necessaria quando tenteremo di accedere al sistema remoto via SSH. Premendo Invio non inseriremo alcuna passphrase, anche se si tratta di una pratica sconsigliabile per ragioni di sicurezza. Una volta reinserita la passphrase per conferma, l'operazione di creazione delle chiavi è terminata e nella directory ~/.ssh troveremo sia la chiave privata (id_dsa) che la chiave pubblica (id_dsa.pub) per il nostro utente.

:: Copiamo la chiave pubblica

A questo punto non resta che copiare la chiave pubblica appena creata sul PC A, in modo tale che su questo sia per noi possibile autenticarci senza password. Sul computer B, quindi, lanciamo il comando seguente adattandolo alla nostra specifica configurazione:
ssh-copy-id -i ~/.ssh/id_dsa.pub ale@192.168.1.4
Al posto di ~/.ssh/id_dsa.pub inseriamo il percorso completo della nostra chiave pubblica, nel caso in cui avessimo scelto un percorso differente da quello di default; al posto di ale, quindi, indichiamo il nome dell'utente sul PC A di cui vogliamo assumere l'identità nelle sessioni SSH, mentre al posto di 192.168.1.4 inseriamo l'indirizzo IP del PC A all'interno della nostra LAN. Dopo aver inserito la password dell'utente sul PC A (ale, nell'esempio riportato) la chiave pubblica verrà copiata nel sistema remoto.

:: Miglioriamo la sicurezza del server

Ora che la configurazione delle chiavi è terminata, è giunto il momento di intervenire sulle opzioni del server SSH così da migliorarne la sicurezza. Sul PC A, quindi, apriamo con un editor da root il file di configurazione del server SSH, /etc/ssh/sshd_config: se usiamo l'editor nano, ad esempio, lanciamo il comando "sudo nano /etc/ssh/sshd_config". Nella finestra dell'editor ricerchiamo la riga "PermitRootLogin yes" e cambiamola in "PermitRootLogin no": in questo modo impediremo l'accesso alla macchina all'utente di amministrazione (chi vorrà ottenere i poteri di root, quindi, dovrà prima accedere al sistema con le credenziali di un utente normale e poi fornire la password di root). Dato che ci autenticheremo mediante l'uso delle chiavi, se vogliamo possiamo disattivare del tutto l'accesso tramite password; individuiamo nel file la riga "#PasswordAuthentication yes" e modifichiamola in "PasswordAuthentication no". Fatto questo, salviamo il file premendo Ctrl + O ed Invio ed usciamo dall'editor con Ctrl + X.

:: Prove di connessione

Terminata la configurazione del server, facciamo rileggere le impostazioni al demone SSH lanciando il comando "sudo /etc/init.d/ssh reload". Adesso non rimane che effettuare una prova di connessione. Sul PC B lanciamo il comando ssh seguito dall'indirizzo del PC A, come nell'esempio seguente:
ssh 192.168.1.4
Una volta inserita la passphrase, otterremo l'accesso al sistema remoto attraverso una console di terminale. Se il nome dell'utente con cui lanciamo ssh sul PC B differisce dall'utente di cui vogliamo assumere l'identità sul PC A, aggiungiamo al comando ssh il nome dell'utente del sistema remoto: "ssh ale@192.168.1.4". Inserendo al termine delle opzioni di ssh un qualsiasi comando, questo verrà eseguito e ne sarà visualizzato l'output nella console del PC B (ad esempio, per eseguire il comando top lanciamo "ssh ale@192.168.1.4 top"): si tratta di modo semplice ed immediato per lanciare singoli comandi su una macchina remota, senza dover aprire prima una console di terminale.

```
Generating public/private dsa key pair.
Enter file in which to save the key (/home/a
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/
Your public key has been saved in /home/ale/
The key fingerprint is:
The key's randomart image is:
+--[ DSA 1024]----+
```

Generiamo la coppia di chiavi sul PC che deve collegarsi al sistema remoto.

:: Collegarci da Internet

Negli esempi di queste pagine si è dato per scontato che la connessione ad un PC avvenga all'interno di una rete locale. Se vogliamo attivare un terminale SSH collegandoci al server remoto da Internet, nessun firewall deve bloccare la porta utilizzata dal server SSH. Se la nostra connessione ADSL è gestita da un router, con la sua interfaccia di configurazione apriamo la porta 22 TCP abilitando il port forwarding verso l'IP della macchina su cui è installato il server SSH.

La presentation è Mobile

Usiamo il cellulare come telecomando per le nostre presentazioni

Forse vi sarà capitato di dover fare una presentazione durante una riunione collegando il notebook a un proiettore e di rimanere per tutto il tempo bloccati davanti al PC, persi in continuo saltellamento tra lo schermo del proprio computer e gli sguardi rimbalzanti del pubblico.
Però fare una presentazione in questo modo non è più così chic come qualche tempo fa e c'è sempre il rischio che qualcuno crolli addormentato se il presentatore è troppo concentrato sulle slide.
Ormai la tendenza è di utilizzare un telecomando o comunque un dispositivo di controllo remoto, che permetta a chi presenta di essere più naturale, svincolandosi dal sistema di proiezione, ma chiaramente allestimenti per presentazioni di questo tipo sono più costosi. Tuttavia, se oltre al notebook abbiamo a disposizione anche di un cellulare con Symbian e possiamo creare un collegamento bluetooth tra i due, abbiamo il nostro dispositivo di controllo remoto!
Il software che permette di gestire le presentazioni dal telefonino in questo modo si chiama Amora (code.google.com/p/amora) ed è open source.

Tutti i cellulari Nokia sono supportati, ma la resa grafica dipende dallo schermo.

:: Cosa occorre

Sul notebook occorre avere una distribuzione linux, perché l'applicazione Amora-server gira solo sul pinguino e l'installazione è un classico configure/make/make install, ma è presente anche l'archivio deb per Debian/Ubuntu e derivate.
Nulla vieta di sfruttare una versione live, ma ogni volta andrebbe riconfigurato il server, oppure provare con una macchina virtuale, ma noi consigliamo caldamente o Debian "Lenny" 5.0 o Ubuntu 9.04 (non la 8.04 che, guardacaso, ha dei bug proprio sulla gestione del bluetooth).

Va poi ovviamente configurato il supporto bluetooth (ormai molto semplice con una delle distribuzioni consigliate) e installato sul telefonino la componente Amora-client.
Amora utilizza Python per Symbian per l'applicazione client, quindi solo i telefoni con la Serie 60 possono utilizzarlo. Prima della parte client, va installato Python per S60 (vedi wiki.opensource.nokia.com/projects/Python_for_S60). Poi basta creare una cartella chiamata Python sulla scheda esterna, all'interno della quale va inserito Amora-client e assicurarsi che ci sia il file presenter.py.
Sempre sul sito di Amora è disponibile per il download un pacchetto combinato che contiene sia Python che Amora-client.
Ora siamo pronti!

:: Utilizzo

Per prima cosa, sul notebook da console (admin) va avviato il servizio con un classico "./amora" che dovrebbe visualizzare un messaggio del tipo "Entering main loop..". Poi sul telefonino va avviata la shell di Python e dal menu tramite Options->Run script selezionare presenter.py sulla memoria esterna. Per avviare il collegamento tramite bluetooth, dobbiamo selezionare Options->Search devices e identificare il nostro PC. Ci verrà chiesto di scegliere una porta, ma la proposta di default dovrebbe andare benissimo (basta accettare premendo OK).
Per utilizzare ora il telefonino come un dispositivo da presentazione selezionare Options->Start. A questo punto il nostro schermo dovrebbe diventare completamente bianco, comunicando che il programma è correttamente in funzione. Muovendo ora le frecce del telefono dovrebbe muoversi il mouse sul pc.

Il client si è connesso e dal cellulare è possibile partire con la presentazione.

Apriamo ora una presentazione tramite Impress della suite di OpenOffice. Premendo 8 sul telefonino si dovrebbe vedere la presentazione in modalità full screen e per scorrere le varie diapositive si utilizzano i tasti 4 e 6 corrispondenti a sinistra e destra della tastiera.
E' possibile avere uno screenshot di quello che visualizza il proprio PC in qualunque momento premendo 2, mentre con 9 si può uscire dalla modalità full screen.

Premendo 2 sul cellulare, otteniamo lo screenshot direttamente sul display.

:: Cosa c'è dentro amora

Amora utilizza solo tecnologie linux: per la comunicazione Bluetooth, è stato integrato BlueZ che è lo stack ufficiale di Linux (ed è il vincolo principale per il porting verso altri sistemi operativi); questo significa che se il proprio pc ha il bluetooth funzionante, si potrà usare quasi sicuramente Amora senza particolari problemi per tastiera e mouse, viene utilizzato XTest che è un'estensione di X Window System.

La comunicazione client-server avviene tramite trasmissione di semplici stringhe di testo. Il server è stato scritto in C e sono in cantiere porting per FreeBSD e MacOSX e fa egregiamente il suo mestiere.

Il tastierino del cellulare permette di gestire tutte le funzioni di un telecomando.

Farebbe piacere avere alcuni miglioramenti, come la possibilità di creare dei profili che memorizzino diversi parametri da poter ripescare velocemente con pochi tasti.

E' però presente la gestione di più client per presentazioni di tipo "collaborativo" ed è stato aggiunto il timer per passare in modo automatico da una slide all'altra. Nelle ultime versioni è stato aggiunto anche il supporto per i tablet PC di Nokia (N800/N810) e si parla anche di una versione j2me che non è però disponibile pre-compilata.
Grazie ad Amora un qualunque cellulare con sistema operativo Symbian può diventare con facilità un sofisticato telecomando.